

Abstract

Methods and correspondent nodes to filter IP communications through firewalls in scenarios where dynamic pinholes are created to ensure an appropriate level of security is disclosed. The invention is based on creating a secure and authorized anchor for communications where all the communications are routed through before a firewall performs the packet filtering. A Translator Gateway (TrGW) switches addresses in the header according to a stored Mapping Table and an interface between a CPS (or a SIP proxy) and the TrGW. This interface allows the CPS to request the TrGW to provide bindings data between IP addresses upon session initiation, the TrGW to provide the bindings data to the CPS and the CPS to release the bindings at session release. The firewall accepts incoming packets whose IP address belongs to the pool of addresses of the TrGW. Thus any incoming packet that does not correspond to an existing call will be dropped at the TrGW, and a valid packet will go through the firewall which will verify that the packet is not a malformed message or other attack.